UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,633	12/01/2000	Katsumi Yoshizawa	09812.0681	4183

22852 7590 08/21/2009

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
DURAN, ARTHUR D	
ART UNIT	PAPER NUMBER
3622	

MAIL DATE	DELIVERY MODE
08/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/727,633	YOSHIZAWA, KATSUMI	
	Examiner	Art Unit	
	Arthur Duran	3622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *6/30/09*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9 and 14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9 and 14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 9 and 14 have been examined.

Response to Amendment

The Amendments filed on 6/30/09 are insufficient to overcome the prior rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanter (5,537,314) in view of Postrel (6,594,640) in further view of Mitty (2001/0037453) in view of Challener (6718468).

Claims 9 and 14: Kanter discloses an information processing apparatus, method for processing information concerning electronic commerce in which a customer receiving services offered by a service provider obtains points in accordance with the amount of money having been paid to said service provider, said information processing apparatus comprising:

first communication controlling means for controlling data communication with another information processing apparatus via a first network (Fig. 1);

first recording means for recording information on a plurality of the service providers and information on a plurality of the customers receiving services from said plurality of service providers (Fig. 1);

second communication controlling means for controlling data communication with a financial institution information processing apparatus via a second network (Fig. 1);

payment computing means for computing an amount of money to be refunded to said customer in accordance with the number of the points said customer owns (col 4, lines 59-67; col 7, lines 5-7); and

signal generating means for generating a signal that requests said financial institution information processing apparatus having an account of said customer to transfer a predetermined amount of money to the account of said customer (col 4, lines 59-67; col 7, lines 5-7), wherein:

said first communication controlling means controls communication in which a signal corresponding to the amount of money computed by said payment computing means is sent to an information processing apparatus owned by said customer and a signal corresponding to a desired amount of transfer money is received from the information processing apparatus owned by said customer (col 4, lines 59-67; col 7, lines 5-7); and

said second communication controlling means controls communication in which the signal generated by said signal generating means is sent to said financial institution information processing apparatus and a signal representing completion of processing by said financial institution information processing apparatus is received (col 4, lines 59-67;

col 7, lines 5-7; col 22, lines 20-50; col 22, line 60-col 23, line 2; col 23, lines 25-45; col 27, lines 40-50).

Kanter further discloses key generating means for generating an encryption key for encrypting and decoding communication data (col 17, lines 53-60; col 17, lines 62-67; col 18, line 65-col 19, line 2; col 23, lines 45-55).

Kanter further discloses authenticating means for authenticating said other information processing apparatus with which communication is controlled by said first communication controlling means (col 17, lines 53-60; col 17, lines 62-67; col 18, line 65-col 19, line 2; col 23, lines 45-55).

Kanter further discloses receiving means for receiving a point redemption request for redeeming points owned by said customer for money, said point redemption request including information on the number of points which is desired to be redeemed for money from among the total points owned by said customer (col 4, lines 59-67; col 7, lines 5-7);

transferring means for transferring, to an account of said customer, an amount of money corresponding to the desired number of points in the information included in said point redemption request from among the total points (col 4, lines 59-67);

and updating means for updating the total points corresponding to said customer (col 24, lines 6-18).

Kanter does not explicitly disclose updating means for updating the total points corresponding to said customer by subtracting the desired number of points in the

information included in said point redemption request from the total points owned by said customer.

Since Kanter discloses the customer having a total points and the customer redeeming the points for cash, it is obvious that Kanter would balance the account of the customer after a points redemption.

Kanter does not explicitly disclose e-commerce over an open network.

However, Postrel discloses e-commerce over an open network (Fig. 4; Fig. 5; col 5, lines 31-36; col 1, lines 13-17; col 1, lines 50-53).

Postrel further discloses a point issuing system and point redemption system which are separate from the plurality of service providers (Fig. 5).

Postrel further discloses that all points control, transfer, redemption, tracking services, can be performed by a server or service separate from the user or merchant (Fig. 4; Fig. 5).

Postrel further discloses authenticating the customer (col 11, line 61-col 12, line 1; col 6, lines 3-7).

Postrel further disclose updating means for updating the total points corresponding to said customer by subtracting the desired number of points in the information included in said point redemption request from the total points owned by said customer (col 5, lines 50-60; col 1, lines 13-17).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add Postrel's utilization of merchant's accessible over the Internet to Kanter's utilization of multiple merchants. One would have been

motivated to do this in order to allow Kanter's users to access a wider range of merchants.

Additionally, Kanter further discloses wherein said authenticating means authenticates said other information processing apparatus based on a unique identifier thereof which is received under the control of said first communication controlling means and which is issued from an authority connected to said first network (col 17, lines 53-60; col 17, lines 62-67; col 18, line 65-col 19, line 2; col 23, lines 45-55).

Additionally, Kanter further discloses that a user is uniquely identified (col 4, lines 39-67; col 18, line 62-col 19, line 5) and then issued a unique certificate (col 4, lines 39-67).

Kanter further discloses uniquely identifying the points that are appropriate to different accounts (col 21, line 55-col 22, line 6); transferring unique amounts of points after a user has been identified (col 22, lines 25-32); that specific amounts of credit or points are transferred to the users account and that the unique cash must be transferred to the appropriate institution (col 22, lines 34-41).

Kanter further discloses unqiue wire transfers (col 22, line 60-col 23, line 2); issuing unique point transfers only under specific conditions (col 24, lines 32-40); issuing unqiue, identifiable points transfers to users (col 27, lines 40-50); and uniquely identified awards and points transfers (col 28, lines 35-45).

Kanter further discloses utilizing identifiers (col 31, lines 31-42).

Kanter also discloses joint or common accounts that can be utilized for all aspects of the invention (col 27, lines 60-65).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that Kanter's providing unique point transfer amounts with unique qualities to a user who has been identified can include identifiers related to the user for the point transfer. One would have been motivated to do this in order to better track the utilization of points.

Additionally, Kanter discloses that joint or common accounts can be utilized for all aspects of the disclosure. Therefore, it would be obvious that after a user has been identified, the user can be given access to a common account from which points redemption will occur. One would be motivated to do this in order provide redemption for users utilizing group accounts.

Additionally, Kanter discloses a point account database connected to the point issuing system and the point redemption system for managing the point account (Fig. 1);

An electronic account book database connected to the point redemption system for storing information on the customer and the plurality of service providers (Fig. 1).

Postrel discloses a point account database connected to the point issuing system and the point redemption system for managing the point account (Fig. 1; Fig. 3; Fig. 4; Fig. 5);

An electronic account book database connected to the point redemption system for storing information on the customer and the plurality of service providers (Fig. 1; Fig. 3; Fig. 4; Fig. 5).

Kanter discloses a temporary storing step of temporarily storing money in a pool account from a plurality of service provider accounts to be used for point transfers; and

A transfer step of transferring money across the financial network from the pool account to a customer account belonging to the customer in response to the point transfer (Fig. 1, item 78; col 21, lines 64-col 22, line 6).

Postrel discloses discloses a temporary storing step of temporarily storing money in a pool account from a plurality of service provider accounts to be used for point transfers; and

A transfer step of transferring money across the financial network from the pool account to a customer account belonging to the customer in response to the point transfer (Fig. 4; Fig. 5; col 5, lines 60-67).

Kanter further discloses that money for point transfers can be held in the sponsor's bank account and taken from there and placed in a third party holding account which is managed by the Central Control Center (Fig. 1, item 78, item 12, item 52; col 21, line 64-col 22, line 6):

"(12) A sponsoring company may be billed for pending commission amounts at each point-of-sale purchase made by a participant at their location. The amount may be electronically debited from the sponsoring company's appropriate bank account ,52, 54 through line 38, I/O 46, bus 44 and stored in memory 78 until at least such time as the appropriate cash return policy of the purchase has expired, so as to insure that the commission will be available when the appropriate participant(s) attempt(s) to redeem the commission" (col 21, line 64-col 22, line 6).

Kanter further discloses a variety of ways and manners that can be utilized for the point transferring and money exchange and that multiple variations of different parties can be involved (col 22, lines 34-41; col 28, lines 28-40; col 17, lines 37-45; col 14, line 62-col 15, line 3; and below):

"(15) Financial institution 92 through another communication line 38, and through I/O 46, line 38 may electronically transfer funds to accounts 52, 54. Alternatively this could be accomplished through direct connection of a conventional communication line (not shown), from institution 92 to accounts 52, or 54. This might occur should a participant 82 or 84 have a credit line approved for use by the financial institution with such status being stored in memory 79, or 30, or in the magnetic stripe of the plastic card, and should the participant make a purchase where the program awards used is less than the purchase total is. The participant could choose to pay the balance using the financial institution approved credit line. If so, computer 60 or 24, could verify the participant's proper status and authorize payment from the lending institution to the appropriate sponsoring company's bank account. The financial institution could then send to the participant, a bill or other means for collection as is customary with such lending procedures, or alternatively, center 12 may issue a bill to the participant" (col 23, lines 25-43).

Kanter also discloses that the participant can be rewarded through the sponsoring company via the central control center or also through the sponsoring company via the central control center where an additional step or additional accounts are utilized for the transfer (Fig. 1 and below):

"(12) Furthermore, commissions can be made available to participants immediately, or held in a holding account memory 78, or in a similar account in memory 30, until such time as the sponsoring company desires to release the commission amounts" (col 21, lines 50-60).

Point transfer for cash can be made from the third party's bank account to the user or from the third party bank account to the holding account to the user:

"(13) When a participant makes a sale at location 14 using earned credit that has been posted by a third party credit issuer to his/her account for use at that location, but the actual cash value has not yet been transferred to a holding account, computer 30 may electronically transfer, through bus 26, I/O 32, line 38, the amount used by the sale, from the third party's bank account to the bank account of location 14" (col 22, lines 34-41).

Notice also that the Holding Account (Fig. 1, item 78) functions as a pool account for temporarily storing money from the plurality of service provider account to be transferred to the customer account during transfer (Fig. 1, item 78); and that the Central Control Center (Fig. 1, item 10) functions as the point transfer dealer account for transferring money from the pool account to the customer account across the financial network in response to the point transfer (Fig. 1, item 10).

In another variation, notice, as cited above, that the financial institution or lending institution can represent multiple sponsoring companies. In this case, the Financial/Lending institution (Fig. 1, item 92) acts as the pool account that is

connected to multiple sponsoring companies. Then, the Holding Account (Fig. 1, item 78) acts as the point transfer dealer account.

Notice that the disclosure of Kanter and the accompanying Fig. 1 of Kanter render obvious multiple variations for point transfer and money exchange. Also, notice the multiple connection and communication paths between the various entities in Fig. 1. And, note that the disclosure of Kanter states that different communication paths and different combinations of entities involved in the transactions and transfers can exist.

Therefore, the disclosure of Kanter and Postrel disclose and render obvious a pool account for temporarily storing money from the plurality of service provider account to be transferred to the customer account during transfer, and a point transfer dealer account for transferring money from the pool account to the customer account across the financial network in response to the point transfer.

Additionally, Kanter renders obvious the utilization of database and tables (Fig. 1, Abstract).

Kanter renders obvious service provider IDs, corresponding financial institution IDs and account numbers for said plurality of service providers (Kanter, Fig. 1, 'Company Accounts', 'Company's Bank Account').

Kanter renders obvious a point management table including customer information (Fig. 1, Participant Accounts'), a corresponding number of issued points (Fig. 1, Participant Accounts'; col 19, lines 5-25), dates on which points were acquired (col 19, lines 5-25); dates on which points will expire (col 21, line 63-col 22, line 7; col

22, lines 7-15; col 4, lines 58-63), service provider IDs responsible for the issued points (col 19, lines 5-25), and a redemption rate (col 18, lines 30-40; col 19, lines 5-25).

Also, Postrel further renders obvious the utilization of database and tables (Fig. 5; Fig. 3).

Postrel further renders obvious service provider IDs, corresponding financial institution IDs and account numbers for said plurality of service providers (Fig. 5; col 10, lines 1-10).

Postrel further renders obvious a point management table including customer information, a corresponding number of issued points, dates on which points were acquired; dates on which points will expire, service provider IDs responsible for the issued points, and a redemption rate (Fig. 5; Fig. 3; col 9, lines 47-55).

Kanter discloses the authenticating means cited above.

Kanter does not explicitly disclose that said authenticating means authenticates based on a certificate issued from a predetermined certificate authority connected to said first network.

Kanter does not explicitly disclose a point redemption system for receiving first data encrypted using a public key of the point redemption system from the customer, the first data comprising second data encrypted using a private key of the customer. . .encrypted data comprising another encrypted data within it.

Additionally, Kanter does not explicitly dislcose data encrypted with a first key comprising data encrypted with a second key as well as data not encrypted with a second key (see Applicant amendments and arguments dated 5/22/08).

Also, see Applicant's Specification Figure 8 for an interpretation of the public and private keys.

However, Mitty discloses data encrypted with a first key comprising data encrypted with a second key as well as data not encrypted with a second key (Fig. 6, 7 [140-146, 160-169]). Further, notice that Mitty discloses double encryption and encryption with both a public and private key ([93; 29]) and that Mitty discloses that the enveloped data of Fig. 7 can be public key encrypted ([41]) and the signed data private key encrypted ([64]). Hence, in Figure 7, the Valued Content is double encrypted by a private and public key. And, the Text/First Part and Text/Second Part are encrypted by a first key which is a public key.

Examiner further notes that a variety of data can be substituted for the text and valued content in Mitty's Fig. 6, 7 (Fig. 6, 7).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add Mitty's utilization of double encryption and public key and private key encryption techniques to Kanter's authenticated transmissions. One would have been motivated to do this in order to better give appropriate levels of security to transmissions.

Hence, the prior art renders obvious data encrypted with a first key comprising data encrypted with a second key as well as data not encrypted with a second key.

Additionally, the claim amendments dated 12/23/2008 included the following claim amendment, "and second data <u>including a random password</u>" where "including a random password" was the part added.

Examiner notes that the double encryption of the second data has already been shown as obvious by the prior art. Hence, all that needs to be demonstrated is that the second data can be a random password.

And, Mitty, as shown above, discloses the Applicant's claimed double encryption. And, Mitty shows that the double encryption occurs on "Valued Content" (Figs, 6, 7, "Valued Content"). And, Mitty states that the Valued Content can be a variety of different content that can be considered valuable, "[0146] The valued contents 635 is application specific. In the examples above, this included the text message that the sender 105 desired to send."

And, note that in Mitty the valued contents can be anything that is "application specific" and it can be something as routine as any "text message that the sender desired to send".

And, Kanter discloses user accounts such as participant accounts, company accounts, holding accounts, bank accounts, etc (Fig. 1). And, the accounts of Kanter commonly use passwords. As an example of this, Postrel discloses user accounts, login ids and account passwords (11:62-64). Also, Mitty discloses password protected keys ([30]).

Hence, it is obvious that the account id and passwords can be valued content and protected by the encryption of Mitty. One would be motivated to do this because account ids and passwords are important and private data that warrant security.

Also, the prior art does not explicitly state that the passwords are random passwords. However, Examiner takes Official Notice that random passwords are

obvious, old and well known. It is well known that passwords can be made up by the user or randomly made up by the service providing the account and password. One would be motivated to use a random password to lessen the chance that someone can guess at the password.

As an example of a random password, Challener discloses random passwords. Also, note that Challener discloses that random passwords can be encrypted and also that random passwords can be associated with public/private keys (Abstract; Fig. 2a).

Additionally, on 6/30/09, Applicant added the following features to the independent claims:

"the user certificate system being connected to the open network, the user certificate including a hash value of a public key of the customer encrypted using a private key of the user certificate system; . . .

. . .and a customer account number"

Examiner notes that Applicant's Specification only mentions hash value or hashing at ([49, 81]) of Applicant's PG_PUB. Hence, hashing is given its normal meaning by the Examiner. And, hashing is a standard process in computer processing.

At Applicant's [49] Applicant states, "As a result of the confirmation, when the data is confirmed to be sent from the authenticated customer, a certificate is generated by signing the public key K.sub.p1 of the customer using the private key K.sub.s3 of the user certificate system 3, which means that the hash value of the public key K.sub.p1 is encrypted using the private key K.sub.s3 and is attached to the certificate."

Kanter does not explicitly disclose a hash value of a public key encrypted with a private key.

Also, on page 8 of the Applicant's Remarks dated 6/30/09, Applicant states that Mitty does not disclose a hash value of a public key.

However, Mitty discloses hashing ([33, 67, 122, 126]).

Mitty further disclsoes hashing or digesting:

"[0033] To form a digital signature, a variable-size message is processed according to a "digesting," or one-way function, such as a "hashing," function, to yield a fixed-sized "digest." (A digesting function is a one-way, irreversible transformation in which the digest, though representative of the message, cannot be used to recreate the message.) The digest is then encrypted with a sender's private key to yield a "digital signature" of the message and sender."

Hence, notice in Mitty that the word hash is synonymous with digest.

Mitty further disclsoes that any data can be hashed/digested:

"[0039] digestedData: includes content of any type and a message digest of the content. A process of constructing such a data structure is defined in the standard, which includes mechanisms for identifying the associated digest algorithm."

And, Mitty discloses a hash or digest value of content being encrypted with a private key ([33] preceding). Mitty further discloses a hash/digest value of content that can be encrypted with a private key ([64, 69, 89, 108]).

Mitty further discloses a public key encrypted with a private key ([28]).

Hence, it is obvious that Mitty's public key is a value that can be converted with a hash or digest. Or, it is obvious that Mitty's public key encrypted with a private key can be hashed before being encrypted. And, it is obvious that this double encryption with hashing can be added to Kanter's key's and encryption. One would be motivated to do this to better secure data and data transmissions.

Also, notice that the public key in Mitty can be located or part of a variety of locations/data. For example, public keys can be part of certificates ([35]).

Also, the following is in regards to the ". . .and a customer account number" feature. In Mitty, the signed data of Figs. 6, 7 includes a customer signature which includes a customer account number or customer identifier ([40]).

Response to Arguments

2. Applicant's arguments with respect to claims 9 and 14 have been considered but are not found persuasive.

On 6/30/09, Applicant added the following features to the independent claims:

"the user certificate system being connected to the open network, the user certificate including a hash value of a public key of the customer encrypted using a private key of the user certificate system; . . .

and a customer account number"

Examiner notes that Applicant's Specification only mentions hash value or hashing at ([49, 81]) of Applicant's PG_PUB. Hence, hashing is given its normal meaning by the Examiner. And, hashing is a standard process in computer processing.

At Applicant's [49] Applicant states, "As a result of the confirmation, when the data is confirmed to be sent from the authenticated customer, a certificate is generated by signing the public key K.sub.p1 of the customer using the private key K.sub.s3 of the user certificate system 3, which means that the hash value of the public key K.sub.p1 is encrypted using the private key K.sub.s3 and is attached to the certificate."

Kanter does not explicitly disclose a hash value of a public key encrypted with a private key.

Also, on page 8 of the Applicant's Remarks dated 6/30/09, Applicant states that Mitty does not disclose a hash value of a public key.

However, Mitty discloses hashing ([33, 67, 122, 126]).

Mitty further disclsoes hashing or digesting:

"[0033] To form a digital signature, a variable-size message is processed according to a "digesting," or one-way function, such as a "hashing," function, to yield a fixed-sized "digest." (A digesting function is a one-way, irreversible transformation in which the digest, though representative of the message, cannot be used to recreate the message.) The digest is then encrypted with a sender's private key to yield a "digital signature" of the message and sender."

Hence, notice in Mitty that the word hash is synonymous with digest.

Mitty further disclsoes that any data can be hashed/digested:

"[0039] digestedData: includes content of any type and a message digest of

the content. A process of constructing such a data structure is defined in the standard, which includes mechanisms for identifying the associated digest algorithm."

And, Mitty discloses a hash or digest value of content being encrypted with a private key ([33] preceding). Mitty further discloses a hash/digest value of content that can be encrypted with a private key ([64, 69, 89, 108]).

Mitty further discloses a public key encrypted with a private key ([28]).

Hence, it is obvious that Mitty's public key is a value that can be converted with a hash or digest. Or, it is obvious that Mitty's public key encrypted with a private key can be hashed before being encrypted. And, it is obvious that this double encryption with hashing can be added to Kanter's key's and encryption. One would be motivated to do this to better secure data and data transmissions.

Also, notice that the public key in Mitty can be located or part of a variety of locations/data. For example, public keys can be part of certificates ([35]).

Also, the following is in regards to the ". . .and a customer account number" feature. In Mitty, the signed data of Figs. 6, 7 includes a customer signature which includes a customer account number or customer identifier ([40]).

Conclusion

The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

aa) Kou, Rose, O'Neill disclose double encryption with a public key and private key;

a) Herz (20010014868) discloses utilizing a private key within a public key ([288]); and Wright (6,052,466) discloses relevant features ("Encryption of data packets using a sequence of private keys generated from a public key exchange").

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arthur Duran whose telephone number is (571)272-6718. The examiner can normally be reached on Mon- Fri, 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eric Stamber can be reached on (571) 272-6724. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Arthur Duran
Primary Examiner
Art Unit 3622

/Arthur Duran/
Primary Examiner, Art Unit 3622
8/18/2009